The automorphism group of a self-dual $[72, 36, 16]$ code is not an elementary abelian group of order 8

Martino Borello*

April 29, 2013

Abstract

The existence of an extremal self-dual binary code $\mathcal{C}$ of length 72 is a long-standing open problem. We continue the investigation of its automorphism group: looking at the combination of the subcodes fixed by different involutions and doing a computer calculation with Magma, we prove that $\mathrm{Aut}(\mathcal{C})$ is not isomorphic to the elementary abelian group of order 8. Combining this with the known results in the literature one obtains that $\mathrm{Aut}(\mathcal{C})$ has order ≤ 5.

Keywords: automorphism group, self-dual extremal codes

1 Introduction

A binary linear code of length n is a subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the field with 2 elements. A binary linear code $\mathcal{C}$ is called *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$ with respect to the Euclidean inner product. It follows immediately that the dimension of such a code has to be the half of the length. The *minimum distance* of $\mathcal{C}$ is defined as $d(\mathcal{C}) := \min_{c\in\mathcal{C}}\{\#\{i \mid c_i = 1\}\}$. In [7] an upper bound for the minimum distance of self-dual binary linear codes is given. Codes achieving this bound are called *extremal*. The most interesting codes, for various reasons, are those whose length is a multiple of 24: in this case $d(\mathcal{C}) = 4m + 4$, where $24m$ is the length of the code, and they give rise to beautiful combinatorial structures [2]. There are unique extremal self-dual codes of length 24 (the extended binary Golay code $\mathcal{G}_{24}$) and 48 (the extended quadratic residue code QR_{48}) and both have a fairly big automorphism group (namely $\mathrm{Aut}(\mathcal{G}_{24}) \cong M_{24}$ and $\mathrm{Aut}(QR_{48}) \cong \mathrm{PSL}_2(47)$). For nearly forty years many people are trying, unsuccessfully, to find a self-dual code of length 72 [9]: a usual approach to this

*M. Borello is with the Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano Bicocca, 20125 Milan, Italy, e-mail: m.borello1@campus.unimib.it. Member of INdAM-GNSAGA, Italy, and of IEEE

problem is to study the possible automorphism groups. Most of the subgroups of $\mathcal{S}_{72}$ are now excluded: the last result is contained in [4], in which the authors finished to exclude all the non-abelian groups with order greater than 5.

In this paper we prove that the elementary abelian group of order 8 cannot occur as automorphism group of such a code, obtaining the following.

Theorem 1.1. *The automorphism group of a self-dual* $[72, 36, 16]$ *code is either cyclic of order* $1, 2, 3, 4, 5$ *or elementary abelian of order* 4.

The techniques which we use are similar to those of [3]: we know [8], up to equivalence, the possible subcodes fixed by all the non-trivial involution. So we combine them pairwise, checking the minimum distance to be 16, and we classify their sum, up to equivalence. We get only few extremal codes and all of them satisfy certain intersection properties that, with easy dimension arguments, make impossible to sum a third fixed subcode without loosing the extremality.

All results are obtained using extensive computations in Magma [5].

2 Preliminaries

Let $\mathcal{C}$ be a self-dual $[72, 36, 16]$ code such that $\mathrm{Aut}(\mathcal{C}) \cong C_2 \times C_2 \times C_2 = \langle a, b, c \rangle$. By [6] all non trivial elements of $\mathrm{Aut}(\mathcal{C})$ are fixed points free and we may relabel the coordinates so that

$$\begin{aligned} a &= (1,2)(3,4)(5,6)(7,8)\dots(71,72) \\ b &= (1,3)(2,4)(5,7)(6,8)\dots(70,72) \\ c &= (1,5)(2,6)(3,7)(4,8)\dots(68,72) \end{aligned}$$

Definition 2.1. *Let*

$$\begin{aligned} &\pi_a : \{v \in \mathbb{F}_2^{72} \mid v^a = v\} \to \mathbb{F}_2^{36} \\ &(v_1, v_1, v_2, v_2, v_3, v_3, v_4, v_4, \dots, v_{36}, v_{36}) \mapsto (v_1, v_2, \dots, v_{36}) \end{aligned}$$

denote the bijection between the fixed space of a *and* $\mathbb{F}_2^{36}$*,*

$$\begin{aligned} &\pi_b : \{v \in \mathbb{F}_2^{72} \mid v^b = v\} \to \mathbb{F}_2^{36} \\ &(v_1, v_2, v_1, v_2, v_3, v_4, v_3, v_4 \dots, v_{35}, v_{36}) \mapsto (v_1, v_2, \dots, v_{36}) \end{aligned}$$

denote the bijection between the fixed space of b *and* $\mathbb{F}_2^{36}$ *and*

$$\begin{aligned} &\pi_c : \{v \in \mathbb{F}_2^{72} \mid v^c = v\} \to \mathbb{F}_2^{36} \\ &(v_1, v_2, v_3, v_4, v_1, v_2, v_3, v_4 \dots, v_{35}, v_{36}) \mapsto (v_1, v_2, \dots, v_{36}) \end{aligned}$$

denote the bijection between the fixed space of c *and* $\mathbb{F}_2^{36}$*.*

Remark 2.2. *The centralizer* $C_{\mathcal{S}_{72}}(a) \cong C_2 \wr \mathcal{S}_{36}$ *of* a *acts on the set of fixed points of* a*. Using the isomorphism* π_a *we hence obtain a group epimorphism which we again denote by* π_a

$$\pi_a : C_{\mathcal{S}_{72}}(a) \to \mathcal{S}_{36}$$

with kernel C_2^{36}. Similarly we obtain the epimorphisms

$$\pi_b : C_{\mathcal{S}_{72}}(b) \to \mathcal{S}_{36}$$

and

$$\pi_c : C_{\mathcal{S}_{72}}(c) \to \mathcal{S}_{36}.$$

If $\mathcal{C}$ is a code and $g \in \mathrm{Aut}(\mathcal{C})$, we denote with $\mathcal{C}(g)$ the subcode of the words fixed by g.

By [8] we have that all the projections of the fixed codes $\pi_a(\mathcal{C}(a))$,$\pi_b(\mathcal{C}(b))$ and $\pi_c(\mathcal{C}(c))$ are self-dual $[36, 18, 8]$ codes. Such codes have been classified in [1], up to equivalence (under the action of the full symmetric group $\mathcal{S}_{36}$) there are 41 such codes. Notice that

$$\langle \pi_a(b), \pi_a(c) \rangle = \langle \pi_b(a), \pi_b(c) \rangle = \langle \pi_c(a), \pi_c(b) \rangle = \langle x, y \rangle \leq \mathcal{S}_{36},$$

with

$$x = (1, 2)(3, 4) \dots (35, 36)$$

and

$$y = (1, 3)(2, 4) \dots (34, 36),$$

are contained respectively in $\mathrm{Aut}(\pi_a(\mathcal{C}(a)))$, $\mathrm{Aut}(\pi_b(\mathcal{C}(b)))$ and $\mathrm{Aut}(\pi_c(\mathcal{C}(c)))$. Only 14 up to the 41 codes, say $\mathcal{Y} := \{Y_1, \dots, Y_{14}\}$, have an automorphism group which contains at least one subgroup conjugate to $\langle x, y \rangle$.

By direct calculation on these 14 codes we get the following conditions on the intersection of the codes.

Lemma 2.3. *Let*

$$(x', y', z') \in \{(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)\}.$$

Then we have only the following possibilities:

$\dim(\mathcal{C}(x') \cap \mathcal{C}(y') \cap \mathcal{C}(z'))$	$\dim(\mathcal{C}(x') \cap \mathcal{C}(y'))$	$\dim(\mathcal{C}(x') \cap \mathcal{C}(z'))$
5	9	9
5	9	10
6	9	9
6	9	10
6	9	11
6	10	10
6	10	11

Let

$$\mathcal{G} := C_{\mathcal{S}_{72}}(\mathrm{Aut}(\mathcal{C})) := \{t \in \mathcal{S}_{72} \mid ta = at, tb = bt, tc = ct\}$$

denote the centralizer of $\mathrm{Aut}(\mathcal{C})$ in $\mathcal{S}_{72}$. Then $\mathcal{G}$ acts on the set of extremal self-dual codes with automorphism group $\langle a, b, c \rangle$ and we aim to find a system of orbit representatives for this action. Here we have some differences with the non-abelian cases, since the full group $\langle a, b, c \rangle$ is a subgroup of the automorphism

group of all the fixed subcodes $\mathcal{C}(a), \mathcal{C}(b)$ and $\mathcal{C}(c)$. The main property that we use is the following, which is straightforward to prove:

$$\pi_a(\mathcal{C}(a))(x) = \pi_b(\mathcal{C}(b))(x) \tag{1}$$

and similar relations for the other fixed subcodes. This allows to combine properly $\mathcal{C}(a)$ and $\mathcal{C}(b)$ classifying their sum.

3 Description of the calculations

Let

$$\mathcal{D} := \{D = D^{\perp} \leq \mathbb{F}_2^{36} \mid d(D) = 8,\ \langle x, y\rangle \leq \mathrm{Aut}(D)\}.$$

The group

$$\mathcal{G}_{36} := C_{\mathcal{S}_{36}}(\langle x, y\rangle) = \pi_a(\mathcal{G}) = \pi_b(\mathcal{G}) = \pi_c(\mathcal{G})$$

acts, naturally, on this set.

Lemma 3.1. *A set of representatives of the $\mathcal{G}_{36}$-orbits on $\mathcal{D}$ can be computed by performing the following computations on each $Y \in \mathcal{Y}$:*

- *Let $x_1, \ldots, x_s$ represent the conjugacy classes of fixed point free elements of order 2 in $\mathrm{Aut}(Y)$.*
- *Compute elements $\tau_1, \ldots, \tau_s \in \mathcal{S}_{36}$ such that $\tau_k^{-1} x_k \tau_k = x$ and put $Y_k := Y^{\tau_k}$ so that $x \in \mathrm{Aut}(Y_k)$.*
- *For every Y_k, consider the set of fixed point free elements $\tilde{y}$ of order 2 in the centralizer $C_{\mathrm{Aut}(Y_k)}(x)$ of x in $\mathrm{Aut}(Y_k)$ such that $\langle x, \tilde{y}\rangle$ is conjugate to $\langle x, y\rangle$ in $\mathcal{S}_{36}$. Let $y_1, \ldots, y_{t_k}$ represent the $C_{\mathrm{Aut}(Y_k)}(x)$-conjugacy classes in this set.*
- *Compute elements $\sigma_1, \ldots, \sigma_{t_k} \in C_{\mathcal{S}_{36}}(x)$ such that $\sigma_l^{-1} y_l \tau_l = y$ and put $Y_{k,l} := Y_k^{\sigma_l}$ so that $\langle x, y\rangle \leq \mathrm{Aut}(Y_{k,l})$.*

Then $\mathcal{D}' := \{Y_{k,l} \mid Y \in \mathcal{Y}, 1 \leq k \leq s, 1 \leq l \leq t_k\}$ represent the $\mathcal{G}_{36}$-orbits on $\mathcal{D}$.

Proof. Clearly these codes lie in $\mathcal{D}$.
Since $\mathcal{G}_{36} \leq \mathcal{S}_{36}$, if we consider different elements in $\mathcal{Y}$, say Y and Y', then $Y'_{k',l'}$ is not in the same orbit of $Y_{k,l}$ for any k', l', k, l.
Now assume that there is some $\gamma \in \mathcal{G}_{36}$ such that

$$Y^{\tau_{k'}\sigma_{l'}} = Y^{\gamma}_{k',l'} = Y_{k,l} = Y^{\tau_k \sigma_l}.$$

Then

$$\epsilon := \tau_{k'} \sigma_{l'} \gamma \sigma_l^{-1} \tau_k^{-1} \in \mathrm{Aut}(Y)$$

satisfies $\epsilon x_k \epsilon^{-1} = x_{k'}$, so x_k and $x_{k'}$ are conjugate in $\mathrm{Aut}(Y)$, which implies $k = k'$ (and so $\tau_k = \tau_{k'}$). Now,

$$Y^{\tau_k \sigma_{l'} \gamma} = Y_k^{\sigma_{l'}\gamma} = Y_k^{\sigma_l} = Y^{\tau_k \sigma_l}.$$

Then

$$\epsilon' := \sigma_{l'}\gamma\sigma_l^{-1} \in \mathrm{Aut}(Y_k)$$

commutes with x. Furthermore $\epsilon'\sigma_l\epsilon'^{-1} = \sigma_{l'}$ and hence $l = l'$.

Now let $Z \in \mathcal{D}$ and choose some $\xi \in \mathcal{S}_{36}$ such that $Z^\xi = Y \in \mathcal{Y}$. Then x^ξ is conjugate to some of the chosen representatives $x_k \in \mathrm{Aut}(Y)$ $(i = 1, \ldots, s)$ and we may multiply ξ by some automorphism of Y so that $x^\xi = x_k = x^{\tau_k^{-1}}$. So $\xi\tau_k \in C_{\mathcal{S}_{36}}(x)$ and $Z^{\xi\tau_k} = Y^{\tau_k} = Y_k$. It is straightforward to prove that the element $y^{\xi\tau_k} \in \mathrm{Aut}(Y_k)$ is a fixed point free elements of order 2 in $C_{\mathrm{Aut}(Y_k)}(x)$ such that $\langle x, y^{\xi\tau_k}\rangle$ is conjugate to $\langle x, y\rangle$ in $\mathcal{S}_{36}$. So there is some automorphism $\alpha \in C_{\mathrm{Aut}(Y_k)}(x)$ and some $l \in \{1, \ldots, t_k\}$ such that $y^{\xi\tau_k\alpha} = y_l$. Then

$$Y^{\xi\tau_k\alpha\sigma_l} = Y_{k,l}$$

where $\xi\tau_k\alpha\sigma_l \in \mathcal{G}_{36}$. □

There are 242 such elements. For our purposes we need to modify a little such set: consider the set $\{Y(x) \mid Y \in \mathcal{D}\}$ and take a set of representatives for the action of $\mathcal{G}_{36}$ on this set, say $\mathcal{F} := \{F_1, \ldots, F_m\}$. By calculations $m = 40$. For every $1 \leq i \leq m$ define the set

$$\tilde{\mathcal{D}}_i := \{Y^\epsilon \mid Y \in \mathcal{D}' \text{ such that there exists } \epsilon \in \mathcal{G}_{36} \text{ so that } Y(x)^\epsilon = F_i\}.$$

Clearly $\bigcup_{i=1}^m \tilde{\mathcal{D}}_i$ is still a set of representatives of the $\mathcal{G}_{36}$-orbits on $\mathcal{D}$, but now $Y_j(x)$ and $Y_k(x)$ are equal if Y_j and Y_k belong to the same $\tilde{\mathcal{D}}_i$ and they are not equivalent via the action of $\mathcal{G}_{36}$ if Y_j and Y_k do not belong to the same $\tilde{\mathcal{D}}_i$.

Let

$$\mathcal{D}_{(a,b)_i} = \{\pi_a^{-1}(Y_a) + (\pi_b^{-1}(Y_b))^\beta \leq \mathbb{F}_2^{72} \mid Y_a, Y_b \in \tilde{\mathcal{D}}_i, \beta \in C_{\mathrm{Aut}(Y_b(x))}(\langle x, y\rangle)\}.$$

Remark 3.2. *For a matter of computation is useful to remark that considering $(\pi_b^{-1}(Y_b))^\beta$ with β varying in $C_{\mathrm{Aut}(Y_b(x))}(\langle x, y\rangle)$ is exactly the same as considering $(\pi_b^{-1}(Y_b))^\tau$ with τ varying in a right transversal of*

$$\mathrm{Aut}(Y_b(x)) \cap C_{\mathrm{Aut}(Y_b(x))}(\langle x, y\rangle)$$

in

$$C_{\mathrm{Aut}(Y_b(x))}(\langle x, y\rangle).$$

Lemma 3.3. *The code $\mathcal{C}(a) + \mathcal{C}(b)$ is equivalent, via the action of $\mathcal{G}$, to an element of $\bigcup_{i=1}^m \mathcal{D}_{(a,b)_i}$.*

Proof. By Lemma 3.1 and by construction of $\bigcup_{i=1}^m \tilde{\mathcal{D}}_i$, there exist $i \in \{1, \ldots, m\}$, $Y_a \in \tilde{\mathcal{D}}_i$ and $\bar{\gamma} \in \mathcal{G}_{36}$ such that $\pi_a(\mathcal{C}(a))^{\bar{\gamma}} = Y_a$. Choose $\gamma \in \pi_a^{-1}(\overline{\gamma})$. Then it is easy to observe that

- $\pi_b(\mathcal{C}^\gamma(b))$ is a self-dual $[36, 18, 8]$ code;
- $\langle x, y\rangle \leq \mathrm{Aut}(\pi_b(\mathcal{C}^\gamma(b)))$ (since $\gamma \in \mathcal{G}$);

- $(\pi_b(\mathcal{C}^\gamma(b)))(x) = (\pi_a(\mathcal{C}^\gamma(a)))(x) = F_i$ (as in (1)).

Now, $\{(Y_b)^\beta \mid Y_b \in \tilde{\mathcal{D}}_i,\ \beta \in C_{\mathrm{Aut}(Y_b(x))}(\langle x, y\rangle)\}$ is the set of all the possible such codes, so $(\pi_b(\mathcal{C}^\gamma(b)))(x)$ is one of these codes. □

Remark 3.4. *There are, up to equivalence in the full symmetric group $\mathcal{S}_{72}$, only* 22 *codes in $\bigcup_{i=1}^{m} \mathcal{D}_{(a,b)_i}$ such that the minimum distance is at least* 16*, say $D_1, \ldots, D_{22}$. They are all $[72, 26, 16]$ codes. In particular*

$$\dim(D_i(a) \cap D_i(b)) = 10.$$

Corollary 3.5. *The code $\mathcal{C}(a) + \mathcal{C}(b)$ is equivalent, via the action of the full symmetric group $\mathcal{S}_{72}$, to a code D_i, with $i \in \{1, \ldots, 22\}$.*

We can repeat in a completely analogous way all the procedure for the pair (a, c) and (b, c), interchanging the roles of the elements a, b and c. Then we get the following.

Corollary 3.6. *The codes $\mathcal{C}(a) + \mathcal{C}(c)$ and $\mathcal{C}(b) + \mathcal{C}(c)$ are equivalent, via the action of the full symmetric group $\mathcal{S}_{72}$, to some codes D_j and D_k, with $j, k \in \{1, \ldots, 22\}$.*

This implies that

$$\dim(\mathcal{C}(a) \cap \mathcal{C}(c)) = 10 \quad \dim(\mathcal{C}(b) \cap \mathcal{C}(c)) = 10. \tag{2}$$

Furthermore, by MAGMA calculations we get that

$$\dim(\mathcal{C}(a) \cap \mathcal{C}(b) \cap \mathcal{C}(c)) = 5. \tag{3}$$

Both can be verified by taking all the elements a', b', c' of order 2 and degree 72 in $\mathrm{Aut}(D_i)$ such that $\langle a', b', c'\rangle$ is conjugate to $\langle a, b, c\rangle$ in $\mathcal{S}_{72}$.

To get a contradiction now is enough to observe that (2) and (3) are not compatible with the table in Lemma 2.3. So we conclude the following.

Theorem 3.7. *The automorphism group of a self-dual $[72, 36, 16]$ code does not contain a subgroup isomorphic to $C_2 \times C_2 \times C_2$.*

Acknowledgment

The author likes to express his gratitude to F. Dalla Volta and G. Nebe for the fruitful discussions and suggestions. *Laboratorio di Matematica Industriale e Crittografia* of Trento deserves thanks for the help in the computational part.

References

[1] C. Aguilar Melchor, P. Gaborit, *On the classification of extremal $[36, 18, 8]$ binary self-dual codes.* IEEE Trans. Inform. Theory 54 (2008) 4743-4750.

[2] E. F. Assmuss, H.F. Mattson, *New* 5*-designs*, J. Combin. Theory 6 (1969) 122–151.

[3] M. Borello, *The automorphism group of a self-dual* $[72, 36, 16]$ *binary code does not contain elements of order* 6, IEEE Trans. Inform. Theory 58, No. 12 (2012), 7240–7245.

[4] M. Borello, F. Dalla Volta, G. Nebe, *The automorphism group of a self-dual* $[72, 36, 16]$ *code does not contain* $\mathcal{S}_3$*,* $\mathcal{A}_4$ *or* D_8, arXiv preprint arXiv:1303.4899 (2013).

[5] W. Bosma, J. Cannon, C. Playoust, *The* Magma *algebra system* I*: The user language*, J. Symbol. Comput. 24 (1997) 235–265.

[6] S. Bouyuklieva, *On the automorphisms of order* 2 *with fixed points for the extremal self-dual codes of length* $24m$, Des. Codes Cryptogr. 25 (2002) 5–13.

[7] C.L. Mallows, N.J.A. Sloane, *An upper bound for self-dual codes*, Information and Control 22 (1973) 188–200.

[8] G. Nebe, *An extremal* $[72, 36, 16]$ *binary code has no automorphism group containing* $Z_2 \times Z_4$*,* Q_8*, or* Z_{10}, Finite Fields and their applications 18 (2012) 563–566.

[9] N.J.A. Sloane, *Is there a* $(72; 36)$ $d = 16$ *self-dual code?*, IEEE Trans. Inform. Theory 2 (1973) 251.